Improved Single Keyword Pattern Matching Algorithm for Intrusion Detection System

Abstract

With the spreading of the internet and online procedures requesting a secure channel, it has become an inevitable requirement to provide the network security. It is very clear that firewalls are not enough to secure a network completely because the attacks committed from outside of the network are stopped whereas inside attacks are not. This is the situation where intrusions detection systems (IDSs) are in charge. IDSs are used in order to stop attacks, recover from them with the minimum loss or analyze the security problems. String matching algorithms are essential for IDS that filter packets and flows based on their payload. This work describes the concept of single keyword pattern matching algorithms. A new improved single keyword pattern matching algorithm is proposed. The new method reduces character comparisons, faster and more reliable in network security applications. The experimental results show that the new algorithm is highly efficient. Its search time is cut down significantly compared with other popular existing algorithms and its memory occupation stays at a low level. Moreover, conclusion on results is made and direction for future works is presented.

References

**Index Terms**

Computer Science

Security

**Keywords**

Network Security  Pattern matching  Intrusion Detection